丢番图方程与判别素数的充要条件

●●黄飞燕　王云葵

摘　要　本文利用丢番图方程获得了判别素数的充要条件,从而获得了默森尼数和费尔马数为素数的充要条件。

1　关于判别素数的充要条件

怎样判别素数? 是数学家们颇为关心的问题,古往今来,国内外数学家都为寻求素数公式或探讨判别素数的充要条件而费尽心思,但至今尚未获得非常有效的方法。1950 年,居加(G·Giuga)猜想[1]: p 为素数的充要条件是

$$1^{P-1}+2^{P-1}+\cdots+(p-1)^{P-1}=-1 \pmod p$$

1932 年,莱梅(Lehmer,D.H.)猜想[2]: p 为素数的充要条件是 $\varphi(p) \mid p-1$。

对此,已有很多人作了深入的研究,并获得了深刻的结论及其等价命题,但尚未彻底解决。另外,作者之一已获得了等幂和与判别素数的充要条件及伯努利(Bernoulli)数与判别素数的充要条件;本文独辟蹊径,利用丢番图方程来研究素数的判别问题,从而获得了费尔马数和默森尼数为素数的充要条件。

定理 1　$N>1$,则 $2N+1$ 为合数的充要条件是,丢番图方程

$$2xy+x+y=N \qquad (1)$$

有正整数解。

证明　必要性,设 $2N+1$ 为合数,则 $2N+1=a\cdot b$,因 $N>1$,则 a 与 b 必是大于 1 的奇数,即必存在正整数 m,n 使得 $a=2m+1,b=2n+1$,从而

$2N+1=(2m+1)(2n+1)$,即 $N=2mn+m+n$。

这就证明了丢番图方程(1) 有正整数解 $x=m,y=n$。

充分性,设方程(1) 有正整数解 x,y,则

$$2N+1=2(2xy+x+y)+1=(2x+1)(2y+1)$$

即 $2N+1$ 为合数。

由定理 1 的逆否命题则立即得到

定理 2　$N>1$,则 $2N+1$ 为素数的充要条件是,丢番图方程(1) 没有正整数解。

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

2 默森尼数为素数的充要条件

形如 $M_p = 2^p - 1$(p 为素数)的数称为默森尼(*Mersenne*)数,关于默森尼数的素合性判别,是计算数论的重要课题。类比地,1989 年王健真猜想[3]:

p 为奇素数,则 $N_P = \frac{1}{3}(2^P + 1)$ 为素数。

1992 年,数学家洪伯阳教授举出反例[4]:当 $p = 29$ 时,$N_{29} = 59 \cdot 3033169$ 是合数,从而推翻了王健真猜想!

如何判别 N_P 的素合性,也是数学家们颇为关心的问题。1990 年莫润(*F. Marain*)利用计算机证明了 N_{3539} 是素数。1989 年,*Selfridge* 猜想[5]:如果下面三条中有两条是正确的,那么第三条也正确:(a)$p = 2^k \pm 1$ 或 $4^k \pm 3$;(b)M_P 是素数;(c)N_P 是素数。

引理 1[4] $p > 3$ 为素数,则 M_P 和 N_P 的素因子必形如 $q = 2pk + 1$(k 为自然数)。

定理 3 $p > 3$ 为素数,则 M_P 为合数的充要条件是,丢番图方程

$$p(2pxy + x + y) = 2^{p-1} - 1 \tag{2}$$

有正整数解。

证明 由引理 1,M_P 的素因子必形如 $2pk + 1$,故 M_P 为合数 $\Leftrightarrow$ 存在正整数 x, y 使得 $M_p = 2^p - 1 = (2px + 1)(2py + 1) \Leftrightarrow$ 方程(2)有正整数解 x, y。

定理 4 $p > 3$ 为素数,则 N_P 为合数的充要条件是,丢番图方程

$$3p(2pxy + x + y) = 2^{p-1} - 1 \tag{3}$$

有正整数解。

证明:由引理 1,N_P 的素因子必形如 $2pk + 1$,故 N_P 为合数 $\Leftrightarrow$ 存在正整数 x, y 使得 $N_p = \frac{1}{3}(2^p + 1) = (2px + 1)(2py + 1) \Leftrightarrow$ 方程(3)有正整数解 x, y。

由定理 3、4 的逆否命题则立即得到

定理 5 $p > 3$ 为素数,则 M_P 为素数的充要条件是,丢番图方程(2)没有正整数解。

定理 6 $p > 3$ 为素数,则 N_P 为素数的充要条件是,丢番图方程(3)没有正整数解。

例如 当 $p = 11$ 时,方程 $11(22xy + x + y) = 2^{10} - 1$ 有正整数解 $x = 1, y = 4$,故 M_{11} 为合数,且 $M_{11} = 23 \cdot 89$。而方程 $33(22xy + x + y) = 2^{10} - 1$ 没有正整数解,故 N_{11} 为素数。

4 费尔马数为素数的充要条件

1640 年,法国数学家费尔马(*Fermat*)发现:$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ 都是素数,据此费尔马猜想:任何费尔马数 $F_n = 2^{2^n} + 1$ 都是素数。然而,1732 年,欧拉(*Euler*)举出反例:$F_5 = 641 \cdot 6700417$ 是合数!从而推翻了费尔马猜想。至今,人们尚未找到判别费尔马

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

数为素数的简便判别法。

引理 2[6] $n \geqslant 2$,则 F_n 的素因子形如 $2^{n+2}k+1$。

定理 7 $n \geqslant 2$,则 F_n 为合数的充要条件是,丢番图方程

$$2^{n+2}xy + x + y = 2^{2^n - n - 2} \quad (4)$$

有正整数解,并且有解时,$F_n = (2^{n+2}x+1)(2^{n+2}y+1)$。

证明:由引理 2,F_n 的因子必形如 $2^{n+2}k+1$,故 F_n 为合数 $\Leftrightarrow$ 存在正整数 x、y 使得 $F_n = 2^{2^n} + 1 = (2^{n+2}x+1)(2^{n+2}y+1) \Leftrightarrow$ 方程(4)有正整数解。

定理 8 $n > 2$,s 是满足 $2^n \geqslant (2n+4)s$ 的任一自然数,则 F_n 为合数的充要条件是,丢番图方程

$$2^{n+2}xy + y - x^{2s} = 2^{2^n - (2n+4)s} \quad (5)$$

有正整数解,并且有解时,

$$F_n = p\left(2^{2s(n+2)}y - \frac{(p-1)^{2s} - 1}{p}\right)$$

其中 $p = 2^{n+2}x + 1$。

证明:必要性,设 F_n 为合数,我们对 s 用数学归纳法证明,方程(5)都有解,当 $s=1$ 时,由 F_n 为合数及定理 7 知,必存在正整数 x, k 使得

$$2^{n+2}kx + k + x = 2^{2^n - n - 2} \quad (A)$$

由题设 $2^n \geqslant 2n+4$,$2^n - n - 2 \geqslant n+2$,故 $2^{n+2} \mid k + x$,令 $x + k = 2^{n+2}y$(y 为正整数),将 $k = 2^{n+2}y - x$ 代入(4)有 $2^{n+2}xy + y - x^2 = 2^{2^n - (2n+4)}$,

即当 $s=1$ 时,方程(5)有正整数解 $x, y = a$,即有

$$2^{n+2}xa + a - x^{2m} = 2^{2^n - (2n+4)m} \quad (B)$$

则当 $s = m+1$ 时,由题设 $2^n \geqslant (2n+4)(m+1)$,$2^n - (2n+4)m > n+2$,故必有 $2^{n+2} \mid a - x^{2m}$,令 $a - x^{2m} = 2^{n+2}b$(b 为整数),将 $a = 2^{n+2}b + x^{2m}$ 代入(B)则有

$$2^{n+2}xb + b + x^{2m+1} = 2^{2^n - (n+2)(2m+1)} \quad (C)$$

由于 $2^n - (n+2)(2m+1) \geqslant n+2$,并且 $b + x^{2m} > 0$,故 $2^{n+2} \mid b + x^{2m+1}$,令 $b + x^{2m+1} = 2^{n+2}y$(y 为正整数),将 $b = 2^{n+2}y - x^{2m+1}$ 代入(C)则有

$$2^{n+2}xy + y - x^{2(m+1)} = 2^{2^n - (2m+4)(m+1)} \quad (D)$$

即当 $s = m+1$ 时,方程(5)也有正整数解。

综上可知,对满足 $2^n \geqslant (2n+4)s$ 的任何自然数 s,丢番图方程(5)总有正整数解。

充分性,设方程(5)有正整数解,令 $p = 2^{n+2}x + 1$,则 $2^{(2n+4)S}y(2^{n+2}x+1) - (2^{n+2}x)^{2S} = 2^{2^n}$

$$p(2^{(2n+4)s}y) - (p-1)^{2s} = F_n - 1$$

$$F_n = p\left(2^{2n+4)s}y - \frac{1}{p}((p-1)^{2s} - 1)\right)$$

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

因 $p > 1$,故 F_n 为合数。

由定理 8 立即得到

定理 9 $n > 3$,则 F_n 为合数的充要条件是,丢番图方程

$$2^{n+2}xy + y - x^2 = 2^{2^n - 2n - 4} \tag{6}$$

有正整数解。

定理8和定理9的逆否命题即为费尔马数为素数的充要条件。由此可见,要判别 F_n 的素合性,只须选择适当的 s,判别方程(5)是否有解即可。例如,当 $n = 6$ 时,取 $s = 2$,因为方程 $2^8 xy + y - x^4 = 2^{32}$ 有正整数解 $x = 1071, y = 4814401$,故 F_6 为合数,并且

$F_6 = 274177 \cdot 67280421310721$。

再如当 $n = 7, s = 1$ 时,方程 $2^9 xy + y - x^2 = 2^{110}$ 有正整数解 $x = 116503103764643, y = 21761889840218569$,故 F_7 为合数,并且

$F_7 = 59649589127497217 \cdot 5704689200685129054721$。

参考文献:

〔1〕王云葵 《等幂和与居加猜想的等价命题》 玉林师专学报 1997,18(3)

〔2〕王云葵 《绝对伪素数与莱梅猜想》 数学教学研究 1996 年度优秀论文专辑

〔3〕王健真 《论费尔马大定理》 中国统计出版社 1989

〔4〕洪伯阳 《数学宝山上的明珠》 湖北科学技术出版社 1993

〔5〕曹珍富 《数论中的问题与结果》 哈尔滨工业大学出版社 1996

〔6〕王云葵 《任何费尔马数都是素数或伪素数》 玉林师专学报 1998,19(3)

〔7〕王云葵 《伯努利数与判别素数的充要条件》 广西民族学院学报 1998,4(1)

〔8〕王云葵 《关于判别费尔马数为伪素数的充要条件》 广西民族学院学报 1998,4(4)

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net